

REMARKS

Claims 1-27 are pending. Claims 1, 11, and 18 are in independent form. Claims 28-30 are cancelled. Favorable reconsideration and further examination are respectfully requested.

Claims 1-27 were rejected under 35 U.S.C. 103(a) as allegedly being unpatentable over Balog et al. (US 2002/0022453), hereinafter "Balog", in view of Olnowich (US 5,612,953), hereinafter "Olnowich", and Morimoto (US 7,024,553), hereinafter "Morimoto".

Claim 1

As amended, independent claim 1 relates to a method to communicate with a first network in a first communication mode, receive encrypted data from the first network, decrypt the encrypted data to form unencrypted data, detect that the unencrypted data is intended to be communicated to a second network, store the unencrypted data, switch to a second communication mode after the unencrypted data is stored, and transmit the unencrypted data to the second network in the second communication mode.

The suggested combination of Balog in view of Olnowich and Morimoto does not describe or suggest features recited in claim 1. Further, Balog describes a method for delivering content to a plurality of mobile devices communicatively coupled to each

other via Bluetooth technology and participating in a communication network. Balog describes a content distribution system comprising a service provider, a user having a plurality of target devices communicatively coupled to each other with at least one of the target devices communicatively coupled to a mobile communication network via an access point.

Further, Balog states:

The service provider 12 includes a content server 22 for storing the content for distribution, a target selector 24 for determining a target 16 most suited for reception of the content, and a protocol selector 26 for determining an optimal communication protocol for delivery of the content [0021].

Balog also states:

Based on user preferences defined in a user profile and the user's current location as defined by the access points 20, along with the user device 16 configuration, the content can be routed to the correct user 14, at a specified time, using the most appropriate communication protocol and path to the preferred device 16 [0029].

Thus, as described in Balog, the protocol for communicating with a first network and transmitting to a second network is based on preferences defined in a user profile and is stored in one or more personalization servers.

Olnowich describes storing a message in a buffer until it is received in full and sending it over a switch network to the commanded destination based on the DID (col. 29, lines 44-48). Olnowich also describes storing the message received from the

network in a buffer until it is received in full and converting it to the serial data protocol (col. 29, lines 54-66).

Morimoto describes a method to update an encrypted key in a wireless LAN system employing encryption by a WEP mechanism. Morimoto also describes a method by which an encrypted key generated by a key management server can be delivered to the access point and to the station to update the encrypted keys stored and supervised thereby (col. 11, lines 46-50).

Balog does not describe switching from a first communication mode for communicating with a first network to a second communication mode for communicating with a second network upon detecting that data received from the first network is intended to be communicated to the second network. In contrast, in Balog, the mobile device relies on the communication protocol chosen by the protocol selector in the service provider (figure 1). Thus, in Balog, the device 52 does not switch communication modes upon detecting that data received from the access point 22 is intended to be communicated to device 56 (figure 7), as recited in claim 1. In contrast, the device relies on the protocol chosen by service provider 12 for communication between access point 22 and device 52, and devices 52 and 56.

Olnowich does not remedy this deficiency in Balog. The cited section of Olnowich (col. 29, lines 57-66) describes

switching between serial and parallel communication protocol, upon storing the data. But, neither this section nor any other part of Olnowich suggest transmitting the data from the first network to a second network. In contrast, in Olnowich, data transfer occurs amongst multiple nodes within the same network (figure 1). Further, in the suggested combination of Balog and Olnowich, the communication protocol between the two networks would be chosen by the service provider and not by the device. Thus, the device would not switch communication modes to transmit stored data upon detecting that data received from the access point is intended to be communicated to a second device, as recited in claim 1. In contrast, the device would rely on the protocol chosen by the service provider for communication and transmission of the stored data.

Morimoto does not remedy this deficiency in the suggested combination of Balog and Olnowich. The cited section of Morimoto (col. 7, lines 51-55) describes encryption of the data communication between stations and access points by a system employing the WEP mechanism. But, neither this section nor any other part of Morimoto suggest transmitting the data from the first network to a second network. Also, in the suggested combination of Balog and Olnowich with Morimoto, the communication protocol between the two networks would be chosen by the service provider and not by the device. Thus, the

device, would not switch communication modes to transmit the unencrypted data upon detecting that encrypted data received from the access point that is decrypted and stored, is intended to be communicated to a second device, as recited in claim 1. In contrast, the device would rely on the protocol chosen by the service provider for communication and transmission of the unencrypted data.

Since the suggested combination of Balog in view of Olnowich and Morimoto fails to describe or suggest receiving encrypted data from a first network in a first communication mode, decrypting the data to form unencrypted data, detecting that the unencrypted data is intended to be communicated to a second network, storing the unencrypted data, switching to a second communication mode, and transmitting the unencrypted data to the second network, as recited in claim 1, obviousness has not been established. Accordingly, claim 1 is not anticipated by the suggested combination. Applicant respectfully requests that the rejection of claim 1 and the claims dependent therefrom be withdrawn.

Claim 11

As amended, independent claim 11 relates to an apparatus comprising a multiplexing device operative to switch a connection to the antenna between the first network interface and the second network interface, and a controller operative to

control the multiplexing device to switch the connection in response to detecting data intended to be communicated between the first network and the second network and after the detected data is stored in the memory.

Balog does not describe or suggest a device comprising a controller operative to control a multiplexing device that switches communication modes upon detecting that data received from the access point is intended to be communicated to a second device (figure 7), as recited in claim 11. Balog describes that the protocol for communicating with a first network and transmitting to a second network is based on preferences defined in a user profile and stored in one or more personalization servers. Thus, device 52 does not switch communication modes upon detecting that data received from access point 22 is intended to be communicated to device 56 (figure 7). In contrast, the device relies on the protocol chosen by service provider 12 for communication between access point 22 and device 52, and devices 52 and 56. Thus, Balog does not describe or suggest an apparatus with the features recited in claim 11. Accordingly, Applicant respectfully requests that the rejection of claim 11 and the claims dependent therefrom be withdrawn.

Claim 18

As amended, independent claim 18 relates to an article comprising a machine-readable medium which stores machine-executable instructions, the instructions causing a machine to communicate with a first network via a first wireless communication link in a first communication mode, receive encrypted data from the first network, decrypt the encrypted data to form unencrypted data, detect that unencrypted data is intended to be communicated to a second network, store the unencrypted data, switch to a second communication mode after the unencrypted data is stored, and transmit the unencrypted data to the second network via a second communication link in a second communication mode.

The suggested combination of Balog in view of Olnowich with Morimoto does not describe or suggest features recited in claim 18 for reasons similar to those discussed above with respect to claim 1. Accordingly, anticipation is not established. Applicant respectfully requests that the rejection of claim 18 and the claims dependent therefrom be withdrawn.

Each of the dependent claims is also believed to define patentable features of the invention. Each dependent claim partakes of the novelty of its corresponding independent claim and, as such, has not been discussed specifically herein.

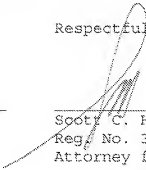
It is believed that all of the pending claims have been addressed. However, the absence of a reply to a specific rejection, issue or comment does not signify agreement with or concession of that rejection, issue or comment. In addition, because the arguments made above may not be exhaustive, there may be reasons for patentability of any or all pending claims (or other claims) that have not been expressed. Finally, nothing in this paper should be construed as an intent to concede any issue with regard to any claim, except as specifically stated in this paper, and the amendment of any claim does not necessarily signify concession of unpatentability of the claim prior to its amendment.

In view of the foregoing amendments and remarks, Applicants respectfully submit that the application is in condition for allowance, and such action is respectfully requested at the Examiner's earliest convenience.

Please apply the 1-Month Extension of Time Fee and  
additional charges or credits to Deposit Account No. 06 1050.

Respectfully submitted,

Date: 8/14/06

  
\_\_\_\_\_  
Scott C. Harris  
Reg. No. 32,030  
Attorney for Intel Corporation

Fish & Richardson P.C.  
Attorneys for Intel Corporation  
PTO Customer No. 20985  
12390 El Camino Real  
San Diego, California 92130  
(858) 678-5070 telephone  
(858) 678-5099 facsimile

10621543.doc